CLAIMS

What is claimed is:

1. A method for transmitting data according to a signature-based protocol comprising:

generating, at a server, a signature corresponding to a signature block, the signature block having a covered data portion and an information object portion, the server conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

storing the signature in the signature block;

transmitting to a client also conversant in the predetermined protocol, the signature block, the signature block further operable to store, in the information object portion, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and corresponding signature without regenerating the signature.

2. The method of claim 1 wherein the signature block further includes a signature value portion, the signature value portion operable to store the signature as an authentication indicator according to the predetermined protocol, wherein storing further comprises storing the signature in the signature value portion.

3. The method of claim 1 wherein the signature block further includes a key information portion, further comprising storing an authentication indicator to a validation instrument in the key information portion, the validation instrument operable to authenticate the signature value portion using the signature.

4. The method of claim 3 wherein the validation instrument corresponds to an inverse operation of the generating of the signature.

5. The method of claim 1 wherein storing in the information object portion further comprises storing the payload data at a client, the client being unencumbered by signature generation operability.

6. The method of claim 1 wherein storing the payload data further comprises generating a transmission block conformant with the predetermined protocol and operable to be received as a signature authenticated transmission by a destination node according to the predetermined protocol.

7. The method of claim 1 wherein generating the signature further comprises generating a signature corresponding to the covered data portion of the signature block.

8. The method of claim 1 further comprising computing a digest on the covered data portion, the digest substantially indicative of the data in the covered data portion.

9. The method of claim 3 wherein the validation instrument is a public key and generating the signature further comprises generating a signature using the private key corresponding to the public key.

10. A method for transmitting data from a nonsigning client according to a signature-based protocol, comprising:

receiving a signature block and a signature corresponding to the signature block, the signature block having a covered data portion corresponding to the signature, and an information object portion, the receiving client conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

storing, in the information object portion of the signature block, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and the corresponding signature without regenerating the signature; and

transmitting, according to the predetermined protocol, the signature block to a recipient destination conversant in the predetermined protocol, the information object portion included in the signature block according to the predetermined protocol.

11. The method of claim 10 wherein the signature block further includes a signature value portion, the signature value portion operable to store the signature as an authentication indicator deterministic of the signature according to the predetermined protocol.

12. The method of claim 10 wherein the signature block further includes a key information portion operable to store an authentication indicator to a validation instrument, the validation instrument operable to authenticate the signature value portion using the signature.

13. The method of claim 10 wherein the receiving is performed by a nonsigning client which does not compute the signature and is unencumbered by components operable to compute the signature.

14. The method of claim 10 wherein receiving the signature further comprises indexing a remote signature repository, and the client is further operable to store the received signature in the signature block according to the predetermined protocol.

15. The method of claim 10 further comprising

receiving an authentication instrument corresponding to the signature, and

storing the received authentication instrument in the signature block with the signed information portion and the signature.

16. The method of claim 15 wherein the received authentication instrument is a public key corresponding to the private key for generating the signature, and storing further comprising forming a self-signed message by storing the public key in the key information portion.

17. The method of claim 13 further comprising:

receiving, at the nonsigning client, a plurality of signatures and corresponding covered data portions;

selecting a first signature for inclusion in a first signature message for transmission to a destination recipient;

selecting a second signature different than the first signature for inclusion in a second signature message for transmission to the same destination recipient.

18. The method of claim 17 wherein selecting the first and second signatures is performed based on signature selection logic, the signature selection logic for analyzing the covered data portion and the information object portion of the signature message to select an expected signature result at the destination recipient.

19. The method of claim 18 wherein the signature selection logic is operable for analyzing the covered data portion based on at least one of the content type, size, creation date, and sparsity of the data.

20. A data communications device for transmitting data according to a signature-based protocol comprising:

a cryptographic engine operable to generate a signature corresponding to a signature block, the signature block having a covered data portion and an information object portion, the server conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

a metalanguage processor conversant in the predetermined protocol and operable to store the signature in the signature block; and

an interface in the data communications device operable to transmit, according to the predetermined protocol, the signature block to a client conversant in the predetermined protocol, the signature block further operable to receive and store, in the information object portion, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and corresponding signature without regenerating the signature.

21. The data communications device of claim 20 wherein the signature block further includes a signature value portion, the metalanguage processor further operable to store, in the signature value portion, authentication indicators according to the predetermined protocol, wherein storing further comprises storing the signature in the signature value portion.

22. The data communications device of claim 20 wherein the signature block further includes a key information portion, the cryptographic engine further operable to store a validation instrument in the key information portion, the validation instrument operable to authenticate the signature.

23. The data communications device of claim 22 wherein the validation instrument corresponds to an inverse operation of the generating of the signature.

24. The data communications device of claim 20 wherein the metalanguage processor is further operable to generate the signature block having the information object portion, the information object portion further operable for storing the payload data at the client unencumbered by signature generation operability.

25. The data communications device of claim 20 wherein the signature block is adapted for storing the payload data by the client to generate a signature message transmission block of data conformant with the predetermined protocol and operable to be received as a signature authenticated transmission by a destination node according to the predetermined protocol.

26. The data communications device of claim 20 wherein the cryptographic engine is further operable to generate the signature corresponding to the covered data portion of the signature block.

27. The data communications device of claim 20 wherein the cryptographic engine is further operable to compute a digest on the covered data portion, the digest substantially indicative of the data in the covered data portion.

28. The data communications device of claim 20 wherein the validation instrument is a public key and generating the signature further comprises generating a signature using the private key corresponding to the public key.

29. A method for transmitting data in a network system according to a signature-based protocol comprising:

identifying, at a server, data adapted for cryptographic transmission;

computing a digest on the identified data, the digest substantially indicative of the identified data;

building, according to a cryptographic scripting language, a signature block, the signature block having a signed data portion, a signature value portion, a key information portion, and at least one information object portion;

storing the identified data in the signed data portion of a signature block;

retrieving, from a public key infrastructure (PKI) a public and private key pair operable for cryptographic operations;

generating, at a server, a signature value from the private key corresponding to the computed digest, the signature substantially unrecreatable by data other than the computed digest;

storing the signature value in the signature value portion of the signature block;

storing the public key corresponding to the private key in the key information portion to provide a self-authenticating transmission; and

transmitting, according to the predetermined protocol, the signature block to a client also conversant in the scripting language and operable to store payload data in the information object portion independently of the signature value portion.

30. The method of claim 29 wherein the scripting language is operable to incorporate signature components such that the scripting language is operable with signing capability when signature components are available and operable without signing capability when signature components are unavailable, further comprising

identifying the signature value portion from a subset of available fields in the signature block, the signature value corresponding to the identified subset and the remaining available fields independent of the signature value;

identifying, from the remaining available fields, payload data portions operable for subsequent storage of data independent of the signature value and the signature value portion, the payload data portions operable to be modified by subsequent recipients, wherein the signature value portion and corresponding signature value persist as a signature block according to the predetermined protocol including the payload data portions.

31. The method of claim 29 further comprising a system for signature use by a nonsigning client, the nonsigning client unencumbered from cryptographic operation components, comprising:

at the client, identifying payload data adapted for storage in the information object portions according to the scripting language independent of the signature value; and

storing the identified payload data in the information object portions in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and corresponding signature without regenerating the signature, the client unencumbered and inoperable to encrypt and decrypt the signed data.

32. A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for transmitting data from a nonsigning client according to a signature-based protocol, comprising:

computer program code for receiving a signature block and a signature corresponding to the signature block, the signature block having a covered data portion corresponding to the signature, and an information object portion, the receiving client

conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

computer program code for storing, in the information object portion of the signature block, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and the corresponding signature without regenerating the signature; and

computer program code for transmitting, according to the predetermined protocol, the signature block to a recipient destination conversant in the predetermined protocol, the information object portion included in the signature block according to the predetermined protocol.

33. A computer data signal for transmitting data from a nonsigning client according to a signature-based protocol, comprising:

program code for receiving a signature block and a signature corresponding to the signature block, the signature block having a covered data portion corresponding to the signature, and an information object portion, the receiving client conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

program code for storing, in the information object portion of the signature block, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and the corresponding signature without regenerating the signature; and

program code for transmitting, according to the predetermined protocol, the signature block to a recipient destination conversant in the predetermined protocol, the information object portion included in the signature block according to the predetermined protocol.

34. A data communications device for transmitting data according to a signature-based protocol comprising:

means for receiving a signature block and a signature corresponding to the signature block, the signature block having a covered data portion corresponding to the

signature, and an information object portion, the receiving client conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;

means for storing, in the information object portion of the signature block, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and the corresponding signature without regenerating the signature; and

means for transmitting, according to the predetermined protocol, the signature block to a recipient destination conversant in the predetermined protocol, the information object portion included in the signature block according to the predetermined protocol.